ZILKA-KOTAB PC

ZILKA, KOTAB & FEECE™

95 SOUTH MARKET ST., SUITE 420
SAN JOSE, CA 95113

TELEPHONE (408) 971-2573
FAX (408) 971-4660

FAX COVER SHEET

Date:	August 19, 2004	Phone Number	Fax Number
To:	Board of Patent Appeals & Interferences, USPTO		(703) 872-9306
From:	Kevin J. Zilka		

Docket No.: NAI1P250_00.024.01 **App. No: 09/593,280**

Total Number of Pages Being Transmitted, Including Cover Sheet: 10

Message:

Please deliver to the Board of Patent Appeals & Interferences.

Thank you,

Kevin J. Zilka

☐ *Original to follow Via Regular Mail* X *Original will Not be Sent* ☐ *Original will follow Via Overnight Courier*

IF YOU DO NOT RECEIVE ALL PAGES OR IF YOU ENCOUNTER
ANY OTHER DIFFICULTY, PLEASE PHONE Erica
AT (408) 971-2573 AT YOUR EARLIEST CONVENIENCE

#14

Practitioner's Docket No. NAI1P250/00.024.01 *PATENT*

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re application of:

Cheuk W. Ko

Art Unit: 2134

Application No. 09/593,280
Filed: 6/13/00

Ex.: Heneghan

For: METHOD AND APPARATUS FOR CONTENT-BASED INTRUSION DETECTION USING AN AGILE KERNEL-BASED AUDITOR

Commissioner for Patents
Alexandria, VA 22313-1450

ATTENTION: Board of Patent Appeals and Interferences

REPLY BRIEF (37 C.F.R. § 1.193)

This Reply Brief is being filed within two (2) months of the mailing of the Examiner's Answer on July 26, 2004.

CERTIFICATION UNDER 37 C.F.R. ' ' 1.8(a) and 1.10*
(When using Express Mail, the Express Mail label number is *mandatory;*
Express Mail certification is optional.)

I hereby certify that, on the date shown below, this correspondence is being:

MAILING

_ deposited with the United States Postal Service in an envelope addressed to the Commissioner for Patents, Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450.

37 C.F.R. § 1.8(a)

_ with sufficient postage as first class mail.

37 C.F.R. § 1.10*

_ as "Express Mail Post Office to Addressee"
Mailing Label No. _____ **(mandatory)**

TRANSMISSION

✓ _ facsimile transmitted to the Patent and Trademark Office, (703) 872-9306.

Date: 8/19/2004

Erica L. Farlow
Signature

Erica L. Farlow
(type or print name of person certifying)

** Only the date of filing (' 1.6) will be the date used in a patent term adjustment calculation, although the date on any certificate of mailing or transmission under ' 1.8 continues to be taken into account in determining timeliness. See ' 1.703(f). Consider "Express Mail Post Office to Addressee" (' 1.10) or facsimile transmission (' 1.6(d)) for the reply to be accorded the earliest possible filing date for patent term adjustment calculations.*

In sections (1) – (9) of the Examiner's Answer, the Examiner recaps the various sections of applicant's appeal brief. Moreover, in section (10), the Examiner states that he is setting forth the rejection of a prior Office Action mailed 10 February 2004.

Thereafter, in section (11), the Examiner sets forth his response to Appellant's previous arguments included in the recently filed appeal brief. Following is an issue-by-issue reply to the Examiner's Answer.

Issue #1 – Group #1

The Examiner argues that appellant's claimed "audit specification" is met by Smaha's disclosed "selected misuses" and "signature data structure." The Examiner goes on to support such assertion by noting that "Appellant's specification only defines an audit specification in that it must have both target attributes and criteria (see specification, page 3, lines 19-23).

In response, applicant emphasizes that the Examiner has selectively gleaned words from applicant's definition and has thus overlooked other components of such definition, in order to argue that applicant's claimed "audit specification" is met by Smaha's "selected misuses" and "signature data structure."

This is improper, as applicant defines the claimed "audit specification" as follows: "This auditing system operates by receiving an audit specification that specifies target attributes to be recorded during an auditing process. The audit specification also specifies an auditing criterion that triggers recording of the target attributes" (emphasis added), not just "target attributes and criteria," as purported by the Examiner.

The Examiner goes on by citing the following new, previously un-cited section of Smaha to meet applicant's claimed "audit specification:"

> "In process flow 100, load mechanism 102 receives selectable misuse data from computer memory device 104 and from storage device 106. Relating FIG. 3 to FIG. 1, computer memory 104 may be thought of as

> computer memory 26. Storage device 28 and load mechanism 102 may be thought of as part of input mechanism 20 for selectable misuses. From these inputs, load mechanism 102 creates signature data structure 108." (see col. 8, lines 11-17)

The Examiner then cites dictionary definitions and concludes that Smaha meets applicant's defined and claimed "audit specification."

Appellant continues to respectfully disagree with this assertion as simply nowhere in the foregoing excerpt or the remaining excerpt is there any sort of attributes to be recorded during an auditing process, nor criterion that triggers recording of the target attributes (emphasis added).

The Examiner continues by rebutting applicant's previous argument below:

> "For example, simply nowhere in Smaha are the "selected misuses" (which are allegedly equivalent to appellant's claimed "audit specification," per the Examiner) used to configure an audit system to produce an audit log which is, in turn, "examin[ed] ... to detect patterns for intrusion detection purposes." While Smaha's "selected misuses" may be used to detect patterns for intrusion detection purposes, they are simply *not* used to configure an audit system to produce an audit log for recording purposes, as claimed. It appears that the Examiner is improperly attempting to use a single entity (i.e. "selected misuses") in Smaha to meet two entities (i.e. "audit specification" and "patterns") in appellant's claims. This obviously fails, especially since the related functionality is not met by Smaha." (see Pages 7-8 of the Appellate Brief)

The Examiner rebuts such arguments by stating that the following output report 42 from Smaha constitutes an audit log.

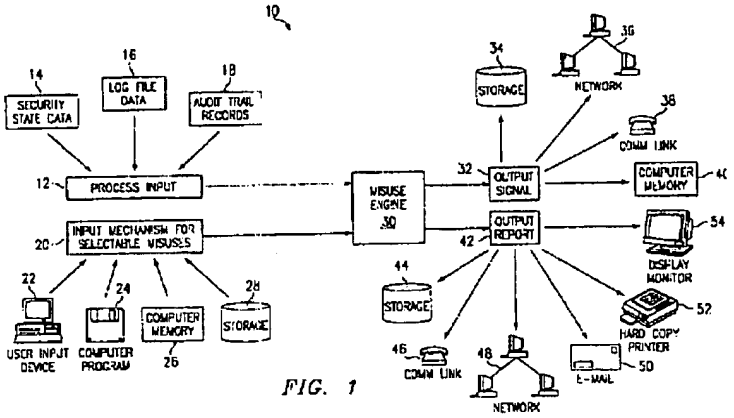

FIG. 1

The Examiner then makes a critical error in improperly assuming that applicant's claimed "examining the audit log to detect patterns for intrusion detection purposes" is met by Smaha, "since Appellant's specification does not discuss the "detection of patterns," and "[n]either Appellant's specification nor Appellant's claims suggest that the audit specification and patterns must be independent of one another."

One need only look at applicant's claim language below to see that the audit specification is used to configure the auditing system to produce an audit log which, in turn, is examined for patterns, two explicitly independent operations:

> "receiving an audit specification;
>
> wherein the audit specification specifies at least one target attribute to be recorded from a set of possible target attributes during an auditing process by the auditing system;
>
> wherein the audit specification also specifies at least one auditing criterion that triggers recording of the at least one target attribute during the auditing process;
>
> configuring the auditing system to record the at least one target attribute in response to detecting the at least one auditing criterion;
>
> running the auditing system to produce an audit log by recording the at least one target attribute in response to detecting the at least one auditing criterion .....
>
> [and]

examining the audit log to detect patterns for intrusion detection purposes"

(emphasis added).

Again, applicant claims two independent operations of using an audit specification to configure the auditing system to produce an audit log, and further examining the audit log for patterns indicative of intrusions.

The Examiner continues by rejecting applicant's arguments regarding the claimed: "wherein a size of the audit log is reduced when the auditing mechanism is run prior to the examination for detection of the patterns." Specifically, the Examiner argues that Smaha need not disclose such language, since it amounts to an intended use and "[i]f the prior art structure is capable of performing the intended use, it meets the claim. In a claim drawn to a process of making, the intended use must result in a manipulative difference as compared to the prior art."

In response, applicant emphasizes that the foregoing functionality goes well beyond an intended use, but also provides for a key functional difference that provides for an enhancement over the prior art. In particular, only applicant teaches and claims "a size of the audit log [that] is reduced when the auditing mechanism is run **prior to** the examination for detection of the intrusion detection patterns." The time of the running of the audit mechanism (and resultant reduced size) relative to the specifically claimed **subsequent** examination for detection of the intrusion detection patterns makes for easier pattern-based intrusion detection, since the audit log is previously reduced in size.

Most importantly, Smaha fails to even suggest, let alone be capable of such specific claimed functional difference.

Finally, with respect to applicant's non-analogous art arguments, it appears that the Examiner has again generalized the description of Borchardt and Smaha to the point that they are analogous. Appellant asserts that such generalization of the descriptions of the arts embodied by Borchardt and Smaha is improper, especially since appellant has clearly set forth the paramount

differences among the particular problems solved in the arts of intrusion detection systems and software buggers.

To simply generalize the arts associated with Borchardt and Smaha to the point that they are "analogous" in order to support the Examiner's obviousness argument, despite the fundamentally different problems which such arts attempt to solve, would frustrate the inventive concepts of appellant, especially in view of the manner in which Borchardt *teaches away* from the concepts of Smaha and would even *frustrate the purpose* thereof.

Issue #1 – Group #2

Regarding the present group, the Examiner argues that "it has been previously noted that the modification of system call jump tables is well-known in the art, both in the initial and final rejections. Appellant has made no attempt to contest this feature's status within the art."

In response, Appellant notes page 15 of AMENDMENT A filed December 11, 2003, where applicant argues:

> "Claims 3, 7, 12, 16, 21, and 25 are rejected under 35 U.S.C. 103(a) as being unpatentable over U.S. Patent No. 5,557,742 to Smaha et al. Specifically, the Examiner has admitted that the subject matter of the instant claims are not disclosed, taught or suggested by Smaha, but then invokes Official Notice regarding such features.
>
> In response, applicant formally requests a specific showing of the subject matter in ALL of the claims in any future action. Note excerpt from MPEP below.
>
> > "If the applicant traverses such an [Official Notice] assertion the examiner should cite a reference in support of his or her position." See MPEP 2144.03."

The Examiner then sets forth definitions of the alleged well-known claimed features, and concludes with a statement that Agrawal teaches the lower layer claimed, and discloses the loading of an interrupt vector table.

Even if the Examiner's assertions above are true, the specifically claimed context of applicant's claimed system call jump table is simply not met.

Specifically, the Examiner has still not met appellant's claimed "auditing system [that] is configured to modify a system call jump table to cause at least one selected system call to execute code that causes the at least one target attribute to be recorded in response to detecting the at least one auditing criterion" (emphasis added). Only appellant teaches and claims an auditing system capable of modifying a system call jump table for the specific purpose of causing a selected system call to execute code that, in turn, causes the at least one target attribute to be recorded in response to detecting the at least one auditing criterion.

Issue #1 – Group #3

Regarding, Group #3, the Examiner has merely incorporated his arguments of Group #2 set forth hereinabove.

Again, the Examiner's rationale fails since applicant has, from the beginning of prosecution, requested a specific prior art showing of applicant's claimed "producing the audit log comprises filtering the at least one target attribute," and the Examiner's rejections fail to address this request. Only applicant teaches and claims the production of an audit log that includes filtering the at least one target attribute.

Issue #2 – Group #1

Regarding this issue and group, the Examiner argues, contrary to applicant's previous assertions, that the Examiner has not admitted that the prima facie case of obvious has not been made.

In response, applicant draws the Examiner's attention to page 6, paragraph 4 of the Final Office Action mailed February 10, 2004, where the Examiner states:

> "Regarding claims 4, 13, 22, Epstein does not completely detail the attributes that are included in system calls, but states that all system calls may be intercepted, along with all associated parameters."

Thus, the Examiner admits that Epstein does not completely detail the attributes that are included in appellant's claimed system calls, and therefore relies on an admittedly deficient prior art showing. By the Examiner's very admission, appellant respectfully asserts that at least the third element of the *prima facie* case of obviousness has not been met, since the references, when combined, fail to teach or suggest all the claim limitations.

Issue #2 – Group #2

Regarding the present issue and group, the Examiner merely makes a blanket statement, without addressing appellant's previously emphasized claim language wherein "the at least one auditing criterion includes ... an identifier for an application program from which the system call is being made." The Unix Programming Environment textbook cited by the Examiner fails to make any mention of appellant's claimed auditing criterion, let alone an auditing criterion that specifically includes an identifier for an application program from which the system call is being made, as claimed.

Appellant respectfully asserts that at least the third element of the *prima facie* case of obviousness has not been met, since the references, when combined, fail to teach or suggest all the claim limitations.

Issue #3 – Group #1

The Examiner responds to the appellant's latest arguments regarding applicant's subject claims by asserting that "Vu discloses such a mechanism for kernel modification for the purpose of detecting system level events that constitute misuses."

Whether this statement is true or not, the Examiner's proposed combination fails to disclose, teach or even suggest the full weight of applicant's claimed manner in which "the auditing system [is configured] to record the at least one target attribute," by specifically using the following three-prong implementation:

> "compiling the audit specification to produce a kernel module;
>
> loading the kernel module into a kernel of an operating system of the computer system; and
>
> linking code from within the kernel module into system calls within the operating system."

Appellant continues to respectfully assert that at least the third element of the *prima facie* case of obviousness has not been met, since the references, when combined, fail to teach or suggest all the claim limitations.

In view of the remarks set forth hereinabove, all of the independent claims are deemed allowable, along with any claims depending therefrom.

In the event a telephone conversation would expedite the prosecution of this application, the Examiner may reach the undersigned at (408) 971-2573. For payment of any additional fees due in connection with the filing of this paper, the Commissioner is authorized to charge such fees to Deposit Account No. 50-1351 (Order No. NAI1P250/00.024.01).

Respectfully submitted,

By: _____ Date: 8/19/04

Kevin J. Zilka
Reg. No. 41,429

P.O. Box 721120
San Jose, California 95172-1120
Telephone: (408) 971-2573